Centre
international
pour la
prévention
de la criminalité

International
Centre
for the
Prevention
of Crime

Centro
Internacional
para la
Prevención
de la Criminalidad

SOMMAIRE EXÉCUTIF

6e Rapport international

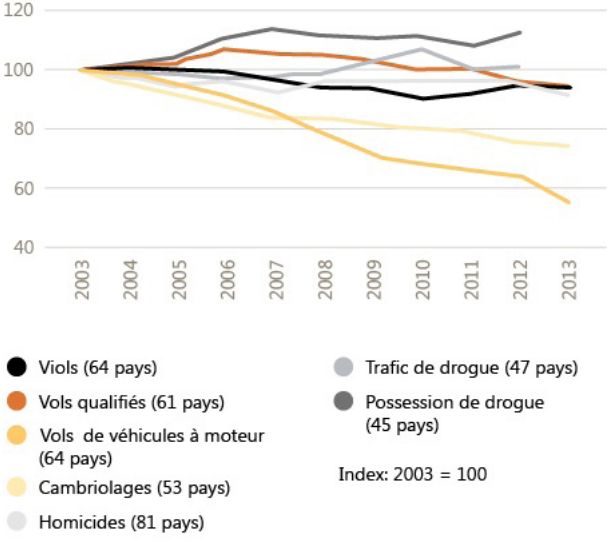
PRÉVENTION DE LA CRIMINALITÉ ET SÉCURITÉ QUOTIDIENNE :
Prévenir la cybercriminalité

SOMMAIRE EXÉCUTIF

Il ressort des travaux menés dans le cadre de l'élaboration des deux derniers Rapports internationaux du CIPC (CIPC, 2014, 2016) qu'en dépit des énormes variations par région et par pays, le taux de crimes traditionnels, exceptés ceux liés aux stupéfiants, n'a pas cessé de reculer depuis 2003.

En revanche, l'importance du cyberespace n'a quant à elle pas cessé d'augmenter. Ce constat fait, nous nous sommes posé la question suivante : existe-t-il une relation entre la baisse des crimes traditionnels et l'importance croissante du cyberespace ? Il semblerait que la diminution des crimes à l'échelle mondiale n'implique pas forcément une tendance vers la disparition de ce type de criminalité, mais plutôt une transformation de cette dernière, les crimes migrant ainsi vers le cyberespace. Cette hypothèse est toutefois difficile à prouver en raison du manque de connaissances sur le sujet. Comme nous allons le voir dans le chapitre 2, les données actuelles dépendent fortement des entreprises privées et de leur agenda économique. Les catégories utilisées pour définir un « crime » ou une « victime » sont larges, fort discutées, et dépendent exclusivement de l'information donnée par les clients. Les échantillons ne sont donc pas représentatifs de la réalité mondiale.

Graphique 1. **Tendances observées dans le monde pour certains crimes, 2003-2013**



Source: ONUDC (2015)

Bien que cette hypothèse semble difficile à prouver, il est impossible de nier l'importance du cyberespace sur la vie quotidienne et contemporaine des personnes, et particulièrement sur le crime. En effet, la cybercriminalité représente aujourd'hui bien plus qu'une simple problématique émergente, en s'imposant comme un enjeu majeur dans la plupart des pays du monde. Dans ce contexte, la prévention de la cybercriminalité devient un besoin immédiat. Est-il possible de prévenir la cybercriminalité ? Existe-t-il des modèles ou cadres de prévention à ce sujet ? Comme dans le cas de la criminalité traditionnelle ou d'autres phénomènes tels que la radicalisation menant à la violence, la prévention a été une réponse tardive à la cybercriminalité. La discussion a en effet davantage été axée sur la cybersécurité et l'empêchement que sur la prévention en tant que telle. En outre, la cybersécurité répond principalement plus aux enjeux de sécurité des entreprises privées et de l'infrastructure numérique que des personnes. En effet, malgré l'évidente difficulté à situer la cybercriminalité dans un espace géographique traditionnel et la tendance à accentuer les facteurs hors-frontières, la plupart des victimes individuelles sont des personnes situées localement. Le défi majeur est donc d'identifier les mécanismes qui permettent d'une part de comprendre le processus de victimisation, et d'autre part, d'activer les meilleures stratégies de prévention à partir de l'interface entre un crime délocalisé et ses victimes locales. La question des victimes individuelles a évidemment été abordée dans le cadre de travaux scientifiques, et il existe à ce sujet des mesures précises de prévention. Cependant, celles-ci se concentrent essentiellement sur les comportements des victimes plutôt que sur les actions des malfaiteurs ou d'autres facteurs criminogènes. Cette approche de prévention est donc très embryonnaire.

Tous ces éléments nous ont conduit à la production d'un Rapport international axé exclusivement sur la question de la prévention de la cybercriminalité, notamment afin d'identifier les lacunes en termes d'informations et d'approches de prévention. À la différence des autres Rapports internationaux, où ont été abordées différentes problématiques autour d'une thématique spécifique, cette édition a été pensée comme un produit complet, chaque chapitre abordant une dimension particulière de la prévention de la cybercriminalité. Comme dans les versions précédentes, le premier chapitre effectue une mise à jour des tendances en matière de prévention de la criminalité en général. C'est donc le chapitre 2 qui introduit spécifiquement la thématique de la cybercriminalité et est considéré comme le chapitre cœur de ce rapport. En effet, le problème de la cybercriminalité y est contextualisé, ainsi que les principales thématiques abordées dans les chapitres suivants. Le chapitre 3 est quant à lui consacré à la cybercriminologie, soit l'étude des cybercrimes, des cybercriminels et des cybervictimes. Le chapitre 4 se penche directement sur la prévention en tant que telle et présente de manière plus détaillée les mesures mises en place et les lacunes d'informations. Enfin, le chapitre 5 aborde une dimension fondamentale de la gouvernance mondiale en matière en prévention de la cybercriminalité : les partenariats public-privés.

Encadré 1. **Rapports internationaux sur la prévention de la criminalité et la sécurité quotidienne : 2008 – 2016**

Les Rapports internationaux précédents ont examiné les tendances en matière de criminalité et d'insécurité, abordé des sujets et des thèmes ciblés, et fait le point sur les tendances en matière de prévention de la criminalité et de sécurité quotidienne.

Thèmes abordés :

2008 : sécurité des femmes, sécurité des jeunes, sécurité dans les écoles, sécurité dans les espaces publics

2010 : migration, crime organisé, drogues et alcool

2012 : trafic humain et exploitation, quartiers informels, zones de post-conflit et de post-catastrophe, production de drogues dans les pays développés

2014 : migration et déplacement des personnes à l'intérieur et à l'extérieur des frontières

2016 : les villes et le Nouvel agenda urbain

Tendances en matière de prévention de la criminalité et sécurité quotidienne

2008 : normes internationales en matière de prévention, réseaux d'échanges internationaux, stratégies nationales et locales ; prévention fondée sur la connaissance ; le rôle des acteurs institutionnels notamment de la police et des acteurs judiciaires ; nouveaux services en soutien à la sécurité quotidienne (sécurité privée, médiation et résolution de conflits) ; élargir le rôle des gouvernements locaux et des acteurs communautaires

2010 : principales tendances en matière de prévention de la criminalité ; bonne gouvernance (décentralisation des pouvoirs, légitimité, réglementation de la sécurité privée, élargissement du rôle de la société civile) ; approches sociales et éducatives ; formation, perfectionnement professionnel et renforcement des capacités ; évaluation de la prévention de la criminalité

2012 : étude mondiale menée sur les stratégies de sécurité dans les villes et leurs composantes

2014 : migration autochtone, prévention de la traite des personnes, violence faite aux femmes dans les relations intimes

2016 : principales tendances en matière de la criminalité et de sa prévention, la sécurité urbaine, territoire et politiques de sécurité publique à partir perspective latino-américaine, les transports publics et la prévention, la consommation de drogues dans un contexte urbain et la radicalisation menant à la violence dans les villes

Thèmes abordés

CHAPITRE 1. Tendances en matière de criminalité et de prévention de la criminalité

Ce premier chapitre cherche à présenter les grandes tendances en ce qui concerne les chiffres sur la délinquance ainsi que les efforts menés à une échelle internationale afin de la prévenir. Il se divise en trois parties. La première partie concerne notamment les tendances internationales en matière de criminalité. Dans ce contexte, nous avons choisi sept thématiques à aborder : les homicides, les homicides de femmes, la violence envers les enfants et les jeunes, la violence dans les villes, les problématiques criminelles liées aux drogues, le taux d'incarcération et le sentiment d'insécurité. La deuxième partie se concentre sur les efforts récents des organismes internationaux et régionaux en matière de prévention de la criminalité, notamment par rapport aux Nations Unies. Enfin, la troisième partie est une description des dernières études empiriques sur le sujet. À ce titre, une revue de littérature des documents scientifiques ayant analysé des données empiriques publiées entre 2015 et 2017 a été réalisée. Celle-ci cherche à décrire l'information la plus récente en matière de prévention de la criminalité et ainsi, présenter un portrait réaliste des intérêts et des préoccupations de la recherche à ce sujet à l'échelle mondiale. Trois thématiques ont été analysées dans ce Rapport : la recherche concernant l'approche communautaire et urbaine, le rôle de la police dans la prévention, notamment l'analyse criminelle et la relation entre les jeunes et la criminalité. Les constats les plus importants de ce chapitre sont les suivants :

- Bien que l'Amérique latine demeure la région au taux d'homicide le plus important au monde, cette violence se concentre dans certains pays de la région, dans certaines villes de ces pays et dans certains secteurs de ces villes. El Salvador et le Honduras sont les pays avec les taux d'homicide les plus élevés au niveau mondial tandis que le Brésil et le Mexique abritent la majorité des villes les plus violentes au monde. En moyenne par pays, 25 % du total des victimes d'homicides en 2015 étaient des femmes. Pour ce qui est de la violence contre les enfants et les jeunes, elle est pratiquement universelle, touchant autant les pays riches que les pays pauvres.

- L'analyse des initiatives des organismes internationaux met en avant l'importance de la coopération et de la coordination entre les pays et entre les régions du monde, liée notamment à un nombre limité de crimes tels que le crime organisé, le terrorisme, la cybercriminalité, le trafic d'êtres humains, les problématiques liées aux drogues, etc. Il a malheureusement été constaté que la plupart des initiatives de coopération ont davantage mis l'accent sur la justice pénale que sur la prévention.

- À partir de la revue de littérature, nous avons pu constater l'importance donnée aux initiatives communautaires et citoyennes de maintien de l'ordre, notamment dans des pays de l'Afrique et de l'Asie. Dans ce cas, ces groupes se focalisent sur la surveillance et le contrôle, en reproduisant ainsi un modèle de police traditionnel. Nous avons également constaté l'importance grandissante de l'analyse criminelle pour la prévention au niveau mondial, notamment au sein des polices et dans les pays d'Amérique du sud. Enfin, des études récentes ont révélé que les actions de prévention et de réinsertion axées sur la punition, l'augmentation de peines et basées sur des approches agressives de la police ne sont pas efficaces pour prévenir la criminalité.

CHAPITRE 2. Les crimes dans un monde numérique

Ce second chapitre tente une problématisation de notre approche des phénomènes de cybercriminalité et se divise en trois volets. Le premier volet ouvre la réflexion autour de la cybercriminalité en s'intéressant à l'environnement spécifique au sein duquel elle s'inscrit, le cyberespace : notamment les dimensions de gouvernance et de facteurs d'inégalités y sont examinées. Le second volet se penche quant à lui sur les difficultés de mesurer la cybercriminalité, des difficultés d'ordre structurel, méthodologique et conceptuel. Enfin, le troisième volet tente, à travers une revue des données et des informations disponibles, d'établir un panorama mondial de la cybercriminalité.

Plusieurs éléments d'intérêt émergent de ce second chapitre :

- Le cyberespace forme un environnement très particulier, aux conditions et aux dynamiques spécifiques, dont plusieurs s'avèrent cruciales pour comprendre les phénomènes cybercriminels. Notamment, la gouvernance particulière du cyberespace décentre les responsabilités de sécurité, de protection, de lutte et de prévention de la criminalité, qui ne relèvent alors plus de l'exclusivité des autorités publiques. Ce « vide de gouvernance » de la sécurité de tous sur Internet constitue l'une des principales opportunités pour la cybercriminalité.

- Le cyberespace forme en outre un milieu différent du monde « réel » : ainsi, les facteurs et les conditions propres au monde « réel » ont une influence sur ceux du monde virtuel, sans pour autant être les mêmes. Ainsi, par exemple, les questions d'inégalités «macro » identifiées dans le monde « réel » (économiques, sociales, de développement, de genre, etc.) ont une influence sur la construction des inégalités virtuelles (d'accès, de compétences et d'usage), mais elles constituent deux systèmes d'inégalité différents.

- Les deux précédents points sont cruciaux dans notre compréhension des phénomènes cybercriminels et de cybervictimisation. En effet, on n'observe pas de corrélation directe entre les dynamiques cyber (criminels comme victimes) et les inégalités observées dans le monde réel ; ce sont des corrélations indirectes, déformées et complexifiées par le prisme du cyberespace. La recherche académique fait ainsi face à un grand défi : repenser les explications du crime dans le monde cyber.

- L'observation de ces activités cybercriminelles est ardue, d'une part en raison de leur grande hétérogénéité, et d'autre part à cause de leur rapide et constante évolution. Cependant, on peut souligner plusieurs aspects clés de cette sphère criminelle, tout particulièrement intéressants du point de vue qui nous intéresse, celui de leur prévention. Premièrement, l'état des connaissances actuelles sur les facteurs favorisant le développement de ces activités, ainsi que ceux favorisant la cybervictimisation, est très embryonnaire. Il apparaît, au regard du corpus très restreint des études sur le sujet, que des corrélations existent entre les facteurs classiques du monde dit « réel » (par exemple décrits dans l'approche écosystémique des facteurs de risque) et la cybercriminalité; pour autant, ces corrélations semblent indirectes, obéissant à des processus et des articulations bien spécifiques, notamment transformées par la transition entre monde réel et cyberespace, ce dernier constituant alors un environnement aux conditions particulières.

- Enfin, on observe de grandes lacunes et une qualité très variable dans les données disponibles. Néanmoins, elles nous permettent de tirer quelques conclusions préliminaires, parmi lesquelles, notamment, une distribution différenciée dans l'espace des différents phénomènes cybercriminels, l'émergence de pôles géographiques de cybercriminalité caractérisés par des activités privilégiées et des modes de gouvernance particuliers.

CHAPITRE 3. Cybercrimes, cyberdélinquants et cybervictimes

Ce troisième chapitre fait l'état des lieux de ce qui se fait aujourd'hui dans la recherche en criminologie sur la cybercriminalité. Qu'entend-on par cybercriminalité? Que sait-on sur les différents cybercrimes? Qui en sont les auteurs et qui en sont les victimes? Autant de questions que les criminologues se posent et pour lesquelles ils cherchent à voir si les théories criminologiques traditionnellement utilisées pour comprendre la délinquance et la victimisation nous sont utiles dans ce nouvel environnement qu'est le cyberespace ou bien s'il est aujourd'hui nécessaire de concevoir une nouvelle approche afin de mieux appréhender ce sujet. Après avoir regardé les différentes perspectives définitionnelles que nous livre la science ainsi que les principales théories appliquées pour comprendre les divers cybercrimes, nous allons par la suite chercher à mieux connaître les avancées de la criminologie sur trois phénomènes en particulier : le piratage informatique, la cyberfraude et les cyberviolences.

Plusieurs constats apparaissent après l'état des lieux qui est fait :

- La définition de la cybercriminalité est source de débat dans le milieu de la recherche. Les cybercrimes sont considérés tantôt comme « du vieux vin dans de nouvelles bouteilles», tantôt comme « du nouveau vin dans de nouvelles bouteilles » et tantôt comme « du vieux vin sans bouteilles ». Dès lors, chaque chercheur choisira une définition en fonction de ses intérêts de recherche faisant en sorte de créer des données très disparates et difficilement comparables.

- Le manque considérable de données sur les victimes individuelles est dû au fait que les personnes ne rapportent pas les faits aux instances compétentes soit par manque de connaissance sur le sujet, soit par crainte que rien ne soit fait du côté de la justice. Du côté des victimes collectives, le faible report est plutôt dû à la crainte de l'impact des cybercrimes sur leur réputation.

- Un profil unique de cybercriminel ou de cybervictimes ne peut absolument pas être développé. Il existe autant de profils qu'il existe de cybercrimes.

- Les théories criminologiques traditionnelles apportent quelques résultats mais il reste encore beaucoup de travail à faire pour mieux appréhender la cybercriminalité. Les chercheurs se penchent d'ailleurs sur la création de nouvelles théories spécifiquement adaptées au cyberespace.

CHAPITRE 4. Quelle prévention pour la cybercriminalité ?

Le cyberespace fait aujourd'hui l'objet d'une nouvelle discussion, tant théorique, que pratique, en matière de prévention de la criminalité. Plusieurs États utilisent les termes de cybersécurité et de cybercriminalité de façon interchangeable et dirigent leurs efforts vers la protection des infrastructures critiques de l'information, au détriment de la nécessaire réflexion entourant la prévention de la criminalité, dans le contexte du cyberespace. En commençant par bien différencier la cybersécurité et la cybercriminalité, tant au niveau conceptuel qu'opérationnel, ce quatrième chapitre a pour objectif de revoir les principaux développements quant aux approches traditionnelles de la prévention de la criminalité, qui sont les approches développementale, environnementale et partenariale, dans ce nouveau contexte. Enfin, il est aussi question d'analyser ces approches dans leur application, à l'aide de différentes mesures prises, dans l'objectif de prévenir certains des crimes les plus souvent cités dans les conventions internationales, soit la cyberintimidation, l'exploitation sexuelle des jeunes en ligne et la cyberfraude. Plusieurs éléments émergent de ce quatrième chapitre:

- Une coopération internationale et multiniveaux : compte tenu de la multitude de facteurs risque et du fait que la cybercriminalité n'est pas assujettie au concept de frontière, sa prévention nécessite une coopération internationale et multiniveaux, tant pour l'harmonisation des cadres légaux, que le partage d'information et de pratiques prometteuses.

- Une approche intégrée : lutter contre ces crimes demande une approche intégrée, menée par différents acteurs, tels le système de justice criminelle, la protection de la jeunesse, l'industrie des technologies de l'information, le milieu scolaire, le secteur de la santé et les services de police, dans une perspective de prévention développementale et environnementale.

- Développement de la connaissance : le développement d'initiatives en prévention de la criminalité nécessite une quantité d'information importante, notamment en ce qui a trait aux facteurs de risque propres à la problématique ciblée. Toutefois, la connaissance entourant les changements entraînés par l'utilisation d'internet, sur les facteurs de risque traditionnels reste encore embryonnaire.

CHAPITRE 5. Les partenariats public-privé en prévention de la cybercriminalité

Ce cinquième et dernier chapitre aborde la question des partenariats public-privé en cybersécurité, et plus spécifiquement la manière dont ils abordent la prévention de la cybercriminalité. En guise d'introduction à la thématique, la première partie a pour objet de définir en quoi consiste un partenariat public-privé, pour ensuite s'attarder sur son émergence en prévention de la criminalité.

La seconde partie dresse un portrait des partenariats public-privé en prévention de la cybercriminalité. Une description des acteurs impliqués dans ces partenariats est présentée, suivie des approches de mise en œuvre et de développement des partenariats, ainsi que leurs composantes. La troisième partie présente un aperçu de partenariats public-privé internationaux et stratégies nationales axés sur la prévention de la cybercriminalité. La quatrième partie se rapporte aux principaux enjeux rencontrés dans le cadre de ces partenariats, et pour conclure la cinquième partie présentent quelques recommandations.

Plusieurs constats peuvent être dégagés de ce chapitre :

- Tel que souligné précédemment dans ce rapport, le cyberespace suppose une gouvernance particulière, qui nécessiterait l'implication d'une diversité d'acteurs pour assumer des responsabilités traditionnellement attribuées au secteur public, telle que la gestion de la sécurité. Le secteur privé se voit ainsi graduellement considéré comme acteur indispensable à la cybersécurité, étant propriétaire des infrastructures qui peuvent non seulement être la cible de cyberattaques, mais qui peuvent également en faciliter la réalisation et la prévention. Cette indispensabilité est toutefois très peu contestée dans la littérature, et l'influence du secteur privé dans la production de connaissances à ce sujet peut soulever certains enjeux.

- Les mesures de prévention mises en œuvre dans le cadre de partenariats public-privé sont majoritairement de l'ordre de la prévention situationnelle, visant principalement la protection des infrastructures critiques. Bien que les connaissances en matière de facteurs explicatifs de la cybercriminalité et de la cybervictimisation demeurent très limitées, les ressources disponibles au sein de partenariats public-privé évoquent tout de même la possibilité que ces derniers puissent contribuer de manière importante à une prévention sociale de ces phénomènes. La mobilisation du secteur privé dans des initiatives de prévention dont les retombées ne sont pas immédiates est toutefois un défi important, comme le démontre l'expérience en prévention de la criminalité.

- Finalement, à certains égards, les enjeux rencontrés dans le cadre de partenariats public-privé en prévention de la cybercriminalité sont semblables à ceux de tout partenariat entre les secteurs public et privé. Une divergence en matière d'identités institutionnelles, d'intérêts, d'attentes et de valeurs perçues comme étant conflictuelles ne sont pas l'apanage du domaine de la cybercriminalité. Toutefois, ces enjeux prennent une dimension nouvelle dans le cyberespace, le secteur privé ayant une mainmise importante sur ce dernier.

Centre international pour la prévention de la criminalité

465, rue Saint-Jean, bureau 803
Montréal (Québec) H2Y 2R6
Canada

+1 514 288-6731

cipc@cipc-icpc.org

Le 6e Rapport international sur la prévention de la criminalité et la sécurité quotidienne est disponible sur le site internet du CIPC www.cipc-icpc.org